UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

WT

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/777,246	12/31/96	OISHI	K 35.G1868

005514 WM31/1105
FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK NY 10112

EXAMINER	
SONG, H	
ART UNIT	PAPER NUMBER
2131	25

DATE MAILED: 11/05/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
08/777,246	OISHI
Examiner	**Art Unit**
Ho S. Song	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *Aug 28, 2001* .

2a) ☒ This action is **FINAL.** 2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-20 and 26-30* is/are pending in the application.

4a) Of the above, claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-20 and 26-30* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☐ Notice of References Cited (PTO-892)
16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____
18) ☐ Interview Summary (PTO-413) Paper No(s). _____
19) ☐ Notice of Informal Patent Application (PTO-152)
20) ☐ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made

2. Claims 1-20,26-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Friedman in view of Merkle(US 5,157,726)..

In claims 1-2,28,30, Friedman teaches inputting first information which could be image file, Private key is stored in the storage and Digital signature is generated based upon the first information (figure 2, page 907). Friedman however, does not teach storing secret key information which fed from an external device and outputting first information containing digital signature and whereby the output information is provided with the digital signature of the person who uses the information input device.. Merkle discloses storing a secret key in an external device and outputs first information containing digital signature whereby output information is provided with the digital signature of the person who uses the information input device in (col.4,

lines 40-46,59-62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to store secret key information in external device as taught in Merkle for storing a private key information internally in the system of Friedman because by storing a secret key information in an external device, it reduces the storage amounts of the system and if whole system is stolen or tampered by unknown attackers, attackers will not have an access to the secret key information because it is stored externally therefore security is greatly strengthen and digital signature ensures image integrity and authenticity. The examiner asserts that it is inherent for Friedman/Merkle's system to include some kind of software/program or set of instructions to reside in the system of Friedman/Merkle to generate digital signature because without any software support, digital signature operation taught in Merkle/Friedman will not be possible.

Claim 10 is rejected based on claims 1-2.

In claims 3,11, Friedman teaches generating a digital signature carries out an operation and outputs digital signature in(figure 2 of page 907).

In claim 4 and 12, Friedman teaches public key cryptography operation in (page 905, third paragraph and figure 1 of page 906).

Claims 6-7 differs from above claims 1-2 in that in claim 6 information is compressed by compressing means. The examiner asserts that it is well known in the art to compress data or information to have faster data transfer rate as well as not reducing the memory capacity. Davies discloses external device stores secret key corresponding to a registered user in(col.5, lines 67).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to store secret key corresponding to a registered user in external device so that only it can filter out from authorized to nonauthorized users therefore security can be enhanced greatly.

In claim 8, Friedman discloses generating carries out an operation and outputs distinguishing information in (fig.2, page 907).

In claims 5,9,13,17, Friedman does not teach using a RSA cryptosytem to obtain a digital signature. The examiner asserts that using RSA cryptosystem to obtain a digital signature is well known art because it's reliable and secure.

As per claim 14, Friedman teaches original message(image file) is inputted from first terminal the examiner asserts that there must be a terminal in order to process image data and second terminal device for having a memory for storing secret information and Friedman discloses an operator for executing a command based on an algorithm for generating a digital signature by using the image data and the secret information in (figure 2 of page 907). The examiner asserts that one of ordinary skill in the art would be motivated to use this scheme because extra security for certification would be provided if two terminal would be used one for storing private key and other for inputting image data instead of having one terminal to perform whole operation. The examiner asserts that it is inherent for Friedman/Merkle's system to include some kind of software/program or set of instructions to reside in the system of Friedman/Merkle

to generate digital signature because without any software support, digital signature operation taught in Merkle/Friedman will not be possible.

As per claim 15, Friedman teaches public key cryptography operation in (page 5, third paragraph and figure 1 of page 906).

As per claim 16, Merkle discloses secret key in (fig.3). One of ordinary skill in the art would be motivated to use secret key because data processing rate is much faster than public key system.

As per claims 18-20, see claims rejection 6-7 above, for discussion of compression techniques in general, further, the examiner asserts that applicant uses well known forms of compression techniques for video data. One skilled in the art would have been motivated to use one of these well known techniques for the advantages they possess.

In claims 26-27 see claim rejection 1-2 above.

In claims 29, Friedman discloses mobile terminal device in (Page 906, digital camera section)

Response to Amendment

7. Applicant has amended claims 1,6,10,14,26 and 27, and added new claims 28-30. Newly added features in the claims has been addressed by the examiner. See above rejection.

Applicant has argued that Friedman does not use the secret key to encode any part of the original image signal. In response: Examiner challenges applicant to show specifically where applicant is claiming **to use secret key to encode any part of the original image signal.** Applicant has argued that in Friedman's reference the private key which is used for the generation of the digital signature is applied only to the hash function and not to the image signal itself and the applicant points in (Page 906, Col.2, lines 4-7) where original message is untouched.

In response: the claim recite " means for using said software to generate a digital signature based upon the first information and the secret key information". It is true that in Friedman, original image is untouched. However, digital signature is generated based upon inputted first information(image file) and the key information. Meaning, first information,hash function and key information are all used to generate digital signature. Friedman's reference specifically discloses outputting first information containing digital signature in (fig.2,page 707). Examiner do not see where applicant is claiming use of secret key to encode first information. Friedman teaches using a private key to generate digital signature rather than secret key disclosed by the applicant. Examiner has previously cited Merkle's patent to address this issue and provided motivation to combine with Friedman's reference in above claims rejection.

Applicant has argued that Merkle's patent fails to disclose the formation of a digital signature by using a secret key to encode at least part of the message being sent. In response:

Examiner do not see where in the claim in which applicant is claiming using a secret to encode message. Examiner challenges applicant to show such a features in the claim. Applicant has argued that neither Friedman nor Merkle shows encoding **at least a portion of the document** with the sender's secret key. In response: these features pointed out by the applicant are not present in the claims.

Conclusion

9 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication should be directed to Ho S. Song at telephone number (703)305-0042. The examiner can normally be reached on Monday through Friday from 6:00 a.m to 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached on (703) 305-9711.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist, whose telephone number is (703) 305-3900.

Ho Song

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100